BAB I

P E N D A H U L U A N

1.1. PENGERTIAN

Sandi adalah bahasa khusus/simbol-simbol/kode-kode yang dibuat supaya suatu informasi yang bersifat rahasia tidak mudah diketahui oleh sebarang orang. Sedangkan ilmu tentang pembuatan, pengkajian dan penguraian isi sandi disebut Kriptografi.

Dalam bahasa Kriptografi terdapat definisi-definisi sebagai berikut :

- Sandi (Cipher) : kode - kode.
- Teks biasa (Plaintext) : pesan yang tidak dikode atau pesan dalam bentuk bahasa/kata yang lazim dipakai sehari-hari.
- Teks sandi (Ciphertext) : pesan yang dikode atau pesan dalam bentuk bahasa atau simbol-simbol yang tidak lazim dipakai.
- Penyandian (Enciphering) : proses pengubahan teks biasa menjadi teks sandi.
- Penguraian (Deciphering) : proses penguraian dari teks sandi ke teks biasa.

Bentuk dan macam sandi sangat banyak ragamnya, ada yang berbentuk huruf-huruf, angka-angka, gambar dan lain-lain. Diantaranya akan diperlihatkan pada contoh di bawah ini.

1'. Sandi Penyulingan (Substitution Ciphers) : dengan prosedur pembuatannya adalah A (dalam teks biasa)

menjadi D (dalam teks sandi), B menjadi E dan seterusnya, seperti terlihat pada bagan berikut ini.

Teks biasa : A B C D E F G .... X Y Z A B C

Teks sandi : A B C D E F G .... X Y Z A B C

Misalnya untuk teks biasa :

BELAJAR JANGAN MENCARI NILAI TETAPI CARILAH ILMU

maka teks sandinya menjadi :

EHODMDUMDQJDQPHQFDULQLODLWHWDSLFDULODKLOPX

(dibuat tanpa spasi)

2'. Sandi Nihilist, sandi yang dipakai kaum Nihilist dari Rusia. Adapun prosedur penyandiannya adalah sebagai berikut :

Pandang tabel di bawah ini.

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

tabel di atas menunjukkan bahwa A (dalam teks biasa) dikonversikan menjadi 11, B menjadi 12, O menjadi 34 dan seterusnya. Jadi berdasarkan baris-kolom. Misalkan akan disandikan kata PULANGLAH dengan kunci kata ANEH , maka:

Teks biasa :	P	U	L	A	N	G	L	A	H
Angka konv.teks biasa:	35	45	31	11	33	22	31	11	23
Angka konv.kunci kata:	11	33	15	23	11	33	15	23	11
Teks sandi yang ter- bentuk. :	46	78	46	34	44	55	46	34	34

Sehingga kata PULANGLAH menurut prosedur sandi Nihilist menjadi : 46 78 46 34 44 55 46 34 34 dengan kunci kata ANEH . Jadi sandi yang terbentuk berupa angka-angka yaitu jumlah angka konversi teks biasa dengan kunci katanya.

Bentuk sandi lain yalni Sandi Hill diciptakan oleh Lester S. Hill. Sandi ini mempunyai karakteristik yang khas dibanding sandi-sandi lainnya, yaitu sistim pembuatannya menggunakan prinsip transformasi matriks. Sehingga sulit bagi orang awam yang tidak memahami hitungan-hitungan matematika khususnya matriks. Sandi Hill inilah yang akan dibahas pada bab selanjutnya.

1.2. PERMASALAHAN

Bagaimana peran matematika di bidang Kriptografi , khususnya sandi Hill yang meliputi penyandian, penguraian sandi dan pemecahan sandi dengan menggunakan matriks, determinan dan hitungan modular.

1.3. PEMBAHASAN

Prinsip pembuatan sandi Hill yaitu dengan mentransformasikan n huruf teks biasa yang berurutan menjadi n huruf teks sandi yang berurutan pula atau sebaliknya menggunakan matrks bujursangkar nxn ; $n \geqslant 2$ dengan elemen bilangan bulat.

Misalnya: $\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$; a_{ij} = bilangan bulat

Dalam pengertian di atas matriks transformasi harus bujursangkar, sebab dari n huruf teks yang berurutan diharapkan hasil transformasinya juga merupakan n huruf yang berurutan. Andaikan matriks transformasinya tidak bujursangkar untuk mentransformasikan matriks kolom dengan 3 baris p_1, p_2, p_3 maka :

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ p_3 \end{bmatrix} = \begin{bmatrix} c_1 = a_{11}p_1 + a_{12}p_2 + a_{13}p_3 \\ c_2 = a_{21}p_1 + a_{22}p_2 + a_{23}p_3 \end{bmatrix}$$

Sehingga setelah dilakukan perkalian matriks menghasilkan matriks kolom dengan 2 baris yaitu c_1 , c_2 (pandang ruas kanan persamaan di atas), sehingga bertentangan dengan yang dikehendaki yaitu hasil transformasi matriks kolom 3 baris tentunya menghasilkan matriks kolom 3 baris. Jadi matriks yang dapat dipakai harus bujursangkar dan dalam hal ini elemen-elemen dalam matriks tersebut hanyalah merupakan bilangan bulat sebarang dan tidak mengandung arti yang khusus. Selanjutnya sandi Hill yang dibuat dengan matriks transformasi (bujursangkar) umuran n x n disebut sandi n-Hill.

Prinsip hitungan modular yang dipakai di sini menggunakan modulo 26, yaitu: a = b (mod.26) ; dikatakan sebagai a setara b modulo 26 atau (a - b) adalah bilangan bulat kelipatan 26. Setiap perhitungan dalam sandi Hill memakai modulo 26.

Sandi yang benar yaitu jika dapat dicari kembali ke dalam bentuknya semula. Karena sandi Hill yang dibicarakan pada sub bab 1.2 menggunakan matriks transformasi ; sebut matriks A, maka matriks tersebut harus mempunyai invers, dalam hal ini invers perkalian modulo 26 . Artinya, jika invers matriks A adalah A^{-1} diperoleh dengan rumus :

$$A^{-1} = |A|^{-1} \ (\text{adj } A)$$

dimana :

$$\text{adj } A = \begin{bmatrix} K_{11} & K_{21} & \cdots & K_{n1} \\ K_{12} & K_{22} & \cdots & K_{n2} \\ \vdots & \vdots & & \vdots \\ K_{1n} & K_{2n} & \cdots & K_{nn} \end{bmatrix}$$

K_{ij} = kofaktor dari a_{ij} dalam A

$= (-1)^{i+j} \ M_{ij}$

M_{ij} = nilai determinan dari matriks bujursangkar A setelah elemen-elemen baris ke-i dan kolom ke-j dihilangkan.

$|A|^{-1}$ = invers perkalian dari $|A|$

maka $|A|^{-1} \ |A| = 1 \pmod{26}$

1.3.1. PENYANDIAN

Prosedur pembentukan teks biasa menjadi teks sandi Hill adalah sebagai berikut :

Langkah 1: Ditentukan dahulu matriks penyandiannya, yaitu matriks bujursangkar n x n dan mempunyai invers perkalian modulo 26.

Langkah 2: Huruf-huruf teks biasa yang berurutan dikelompokkan masing-masing n huruf dan diganti masing-masing huruf dengan nilai numeriknya, sesuai tabel 1 (lihat lampiran).

Langkah 3: Secara berurutan masing-masing kelompok di atas dikonversikan ke matriks kolom p dan dilakukan perkalian matriks.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix}$$

$$\rightarrow \quad A \quad p \quad = \quad c$$

A = matriks transformasi

p = matriks kolom teks biasa

c = matriks kolom teks sandi

Langkah 4: Dicari kembali huruf-huruf yang sesuai dengan c_1 , c_2 , ... , c_n dengan memakai tabel 1.

1.3.2. PENGURAIAN SANDI.

Penguraian teks sandi menjadi teks biasa, terlebih dahulu dicari invers perkalian modulo 26 dari matriks penyandiannya. Kemudian mentransformasikan teks sandi menjadi teks biasa dengan cara seperti dalam penyandian dengan menggunakan matriks invers penyandiannya sehingga berbentuk :

$$\begin{bmatrix} A_{11} & A_{21} & \cdots & A_{n1} \\ A_{12} & A_{22} & \cdots & A_{n2} \\ \vdots & \vdots & & \vdots \\ A_{1n} & A_{2n} & \cdots & A_{nn} \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{bmatrix} = \begin{bmatrix} p_1 \\ p_2 \\ \vdots \\ p_n \end{bmatrix}$$

$$\rightarrow \quad A^{-1} \quad c \quad = \quad p$$

A^{-1} = matriks invers perkalian modulo 26 dari A.

c = matriks kolom teks sandi

p = matriks kolom teks biasa

1.3.1. PEMECAHAN SANDI

Pemecahan sandi yang dimaksud di sini adalah menguraikan isi sandi tanpa diketahui matriks penyandiannya , tetapi hanya diberikan kunci pembacaannya berupa sekelompok kata sandi berikut artinya. Dari kunci pembacaan tersebut dapat dicari matriks pengurainya.